2Ц

УДК 004.382

Е.С. Цыбульник, В.Н. Пигуз
Институт проблем искусственного интеллекта МОН Украины и НАН Украины,
г. Донецк
info@iai.donetsk.ua

Интеллектуальное устройство контроля доступа

В статье предлагается способ усовершенствования устройства контроля доступа с электронными ключами типа DS1990A. Реализация способа позволяет защитить систему от ключей-клонов и ключей-симуляторов при незначительном удорожании системы в целом и без дополнительной нагрузки на пользователей.

Введение

В настоящее время широкое распространение получили системы контроля доступа, основанные на применении электронных ключей (таблеток в бытовом понимании). Принято считать, что каждый ключ уникален чуть ли не в мировом масштабе, его трудно подделать и трудно восстановить при утере. Однако это далеко не так, и далее в статье рассматриваются причины неуникальности ключей и предлагается способ усовершенствования устройства контроля и системы контроля доступа в целом.

1 Устройство и работа электронного ключа

Электронный ключ (Touch Memory) типа DS1990A представляет собой пассивное устройство (без внутреннего источника питания), которое содержит записанное с помощью лазера постоянное запоминающее устройство (ПЗУ). ПЗУ содержит уникальный, 48-битный серийный номер. Для считывания данных с DS1990A используется 1-проводная шина фирмы DALLAS. DS1990A является подчинённым устройством, а мастером является обычно микропроцессор. Питание DS1990A во время обмена данными производится от 1-проводной шины. Эквивалентная схема интерфейсной части DS1990A показана на рис.1а), а на рис.1б) показан вариант подключения линии порта микроконтроллера.

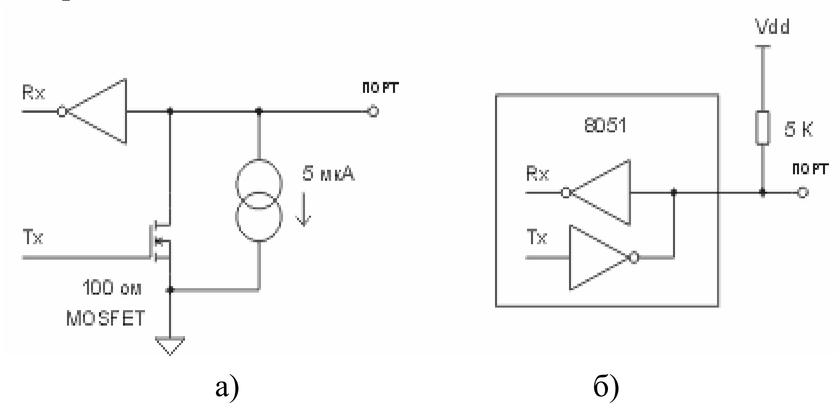


Рисунок 1 – Эквивалентная схема интерфейсной части DS1990A (а) и мастера (б)

В состоянии ожидания 1-проводная шина имеет высокий логический уровень. Последовательность доступа к DS1990A по 1-проводной шине следующая: инициализация, команда чтения ПЗУ, чтение данных.

Все пересылки по 1-проводной шине начинаются с инициализации. Инициализация производится в следующей последовательности (рис. 2):

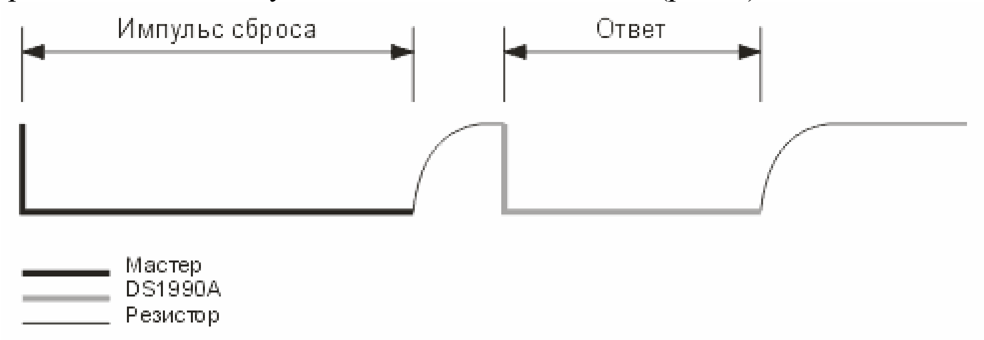


Рисунок 2 – Инициализация обмена по 1-проводной шине

Мастер посылает импульс сброса (reset pulse) – сигнал низкого уровня длительностью не менее 480 мкС и не более 900 мкС.

За импульсом сброса следует ответ подчиненного устройства (presence pulse) – сигнал низкого уровня длительностью 60 – 240 мкС, который генерируется через 15 – 60 мкС после завершения импульса сброса.

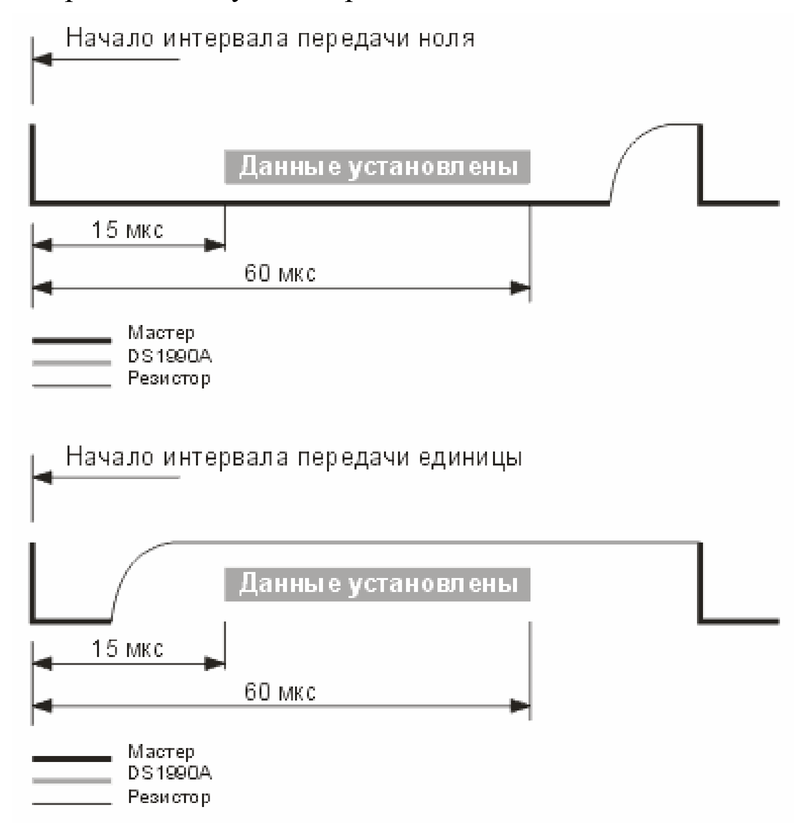


Рисунок 3 – Интервалы записи ноля и единицы по 1-проводной шине

Ответ подчиненного устройства даёт мастеру понять, что на шине присутствует устройство DS1990A и оно готово к обмену. После того как мастер обнаружил ответ, он может передавать команду чтения ПЗУ. Команда чтения ПЗУ имеет шестнадцати-

ричный код 0x33 или 0x0F. Передача данных команды чтения ПЗУ ведётся путём формирования специальных временных интервалов (time slots). Каждый временной интервал служит для передачи одного бита. Первым передаётся младший бит команды. За импульсом низкого уровня следует передаваемый бит. Он должен удерживаться на шине 60 – 120 мкС от начала интервала. Временной интервал завершается переводом шины в состояние высокого уровня на время не менее 1 мкС. Это необходимо для зарядки внутреннего конденсатора, который обеспечивает питание DS1990A. Аналогичным образом формируются временные интервалы для всех передаваемых битов (рис. 3).

2 Программный контроль кода доступа

Приняв команду чтения ПЗУ, DS1990A передает 8-битный код типа устройства (для DS1990A это 01H), 48-битный серийный номер и 8-битную контрольную сумму. Байты серийного номера следуют от младшего к старшему. То есть если на контактной поверхности ключа указаны цифры:

FF 01
00 00 00 13 C0 CA,

то они будут считаны в следующей последовательности:

01 CA C0 13 00 00 00 FF.

При этом биты в каждом байте будут также передаваться от младшего к старшему, т.е. при чтении с линии данных вышеприведенного примера будет получаться следующая последовательность бит:

1000	0000	0101	0011	0000	0011	1100	1000	0000	0000	0000	0000	0000	0000	1111	1111
1	0	A	C	0	C	3	1	0	0	0	0	0	0	F	F

Временные интервалы для принимаемых битов тоже формирует мастер. Интервал начинается импульсом низкого уровня длительностью 1 – 15 мкС. Затем мастер должен освободить шину, чтобы дать возможность DS1990A вывести бит данных. По переходу из единицы в ноль DS1990A выводит на шину бит данных и запускает схему временной задержки, которая определяет, как долго бит данных будет присутствовать на шине. Это время лежит в пределах 15 – 60 мкС. Для того чтобы данные на шине гарантированно установились, требуется некоторое время. Поэтому момент считывания данных мастером должен отстоять чуть больше, чем на 15 мкС от начала временного интервала (рис. 4).

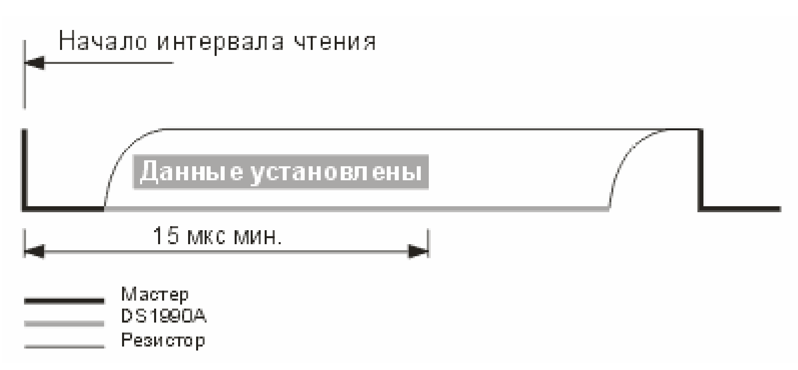


Рисунок 4 – Интервал чтения по 1-проводной шине

Правильность принятых данных контролируется с помощью контрольной суммы. Если подсчитать контрольную сумму (КС) первых семи считанных байтов (т.е. не включая байт считанной контрольной суммы), то в случае отсутствия ошибок считанная КС должна совпадать с вычисленной КС.

Фирма DALLAS (разработчик электронных ключей) предлагает стандартную процедуру вычисления контрольной суммы, текст которой для МК с системой команд x51 приведен ниже:

```
    EXTERN DATA (CRC);// внешняя переменная для CRC.
    mov    a, r7;           // параметр в процедуру передается через r7
    push   acc;             // сохранить аккумулятор.
    push   b;          // Сохранить регистр B.
    push   acc;             // Сохранить сдвигаемые биты.
    mov    b, #8;           // Число сдвигов = 8.
CRC_LOOP:
    xrl    a, CRC;          // Получить новое значение CRC
    rrc    a;               // сдвинуть CRC в перенос
    mov    a, CRC;          // получить последнее значение CRC
    jnc    ZERO;            // пропустить, если data = 0
    xrl    a, #18h;         // обновить значение CRC.
ZERO:
    rrc    a;               // позиционировать новую CRC
    mov    CRC, a;          // сохранить новую CRC
    pop    acc;        // получить оставшиеся биты
    rr     a;               // позиционировать следующий бит
    push   acc;             // сохранить оставшиеся биты
    djnz   b, CRC_LOOP;     // проверка завершения цикла
    pop    acc;        // восстановить аккумулятор
    pop    b;               // восстановить регистр B
    pop    acc;        // восстановить аккумулятор
    ret
```

3 Недостатки работы с электронными ключами

При практическом применении электронных ключей следует учитывать следующие обстоятельства:

– имеется множество производителей клонов DS1990A, например, TL1990A;

– номера ключей для клонов НЕ ЗАВИСЯТ от номеров DS1990A, т.е. имеется потеря такого свойства ключей, как оригинальность номера в мировом масштабе;

– номера ключей в семействе клонов НЕ ЯВЛЯЮТСЯ ОРИГИНАЛЬНЫМИ, т.е. в партии ключей имеется множество ключей с ОДИНАКОВЫМИ НОМЕРАМИ;

– клоны зачастую не выдерживают температурные параметры, что приводит их в нерабочее состояние на морозе (ключи приходится согревать перед использованием).

Кроме того, незащищенность кодовой области ключа позволяет легко скопировать ключ (для этого достаточно 1 С) с помощью довольно простого устройства и также просто сделать симулятор для одного или множества ключей. Наличие надписи с кодом ключа на его лицевой поверхности позволяет получить копию ключа путем простого фотографирования даже с помощью мобильного телефона с последующим занесением кода в устройство клонирования или симулятор ключа.

Таким образом, относительно стандартных электронных ключей типа DS1990A, TL1990A можно сделать следующее предварительное заключение:
простейшие электронные кодовые ключи типа DS1990A, TL1990A не годятся для систем с повышенными требованиями к безопасности, т.к. не обеспечивают ни оригинальности ключа, ни защиты от копирования. Они являются «оригинальными» только для людей, несведущих в электронике и программировании.

4 Способ повышения защищенности контроля доступа

Разумеется, фирма-разработчик электронных ключей прекрасно знает о всех этих недостатках и разработала ряд альтернативных решений. На свет появились электронные ключи с повышенной защитой типа DS1991, DS1992, DS1993 и другие. Имеет смысл привести примерную стоимость этих ключей: DS1990 – $ 1,5, DS1992 – $ 10, DS1993 – $ 12. Кроме того, пользователю таких ключей необходимо приобрести программатор для ключей типа DS1991, DS1992, DS1993... стоимостью более $ 100. Очевидно, что такая система контроля доступа будет уже не простой и не дешевой в эксплуатации.

Однако если в качестве считывающего устройства поставить микроконтроллер, имеющий на борту АЦП и с достаточно большим быстродействием (25 MIPS и более), то можно значительно улучшить защищенность системы контроля доступа.

Достигается это следующим образом. Внутренняя система питания ключа DS1990A не имеет стабилизатора напряжения и выходной полевой транзистор ключа имеет конечное внутреннее сопротивление. Это означает, что уровень «0» при ответе ключа зависит от напряжения внешнего питания, емкости конденсатора и внутреннего сопротивления выходного транзистора ключа. Если измерить значения напряжения в начале фазы ответа ключа – presence pulse, в середине этой фазы и в конце фазы, записать в память системы контроля доступа эти значения вместе с кодом ключа, то эти данные могут служить дополнительными параметрами идентификации ключа.

Для достаточно быстродействующего микроконтроллера можно написать программу, которая не просто задает параметры временных интервалов (time slots) при чтении данных ключа, но и изменяет их при записи данных ключа в систему доступа. При этом записываются данные, которые соответствуют минимальной длительности time slots. Тогда чтение данных ключа можно проводить в три этапа: при первом чтении используются стандартные временные параметры, извлекаются дополнительные данные для этого конкретного ключа, производится повторное чтение данных с минимальными значениями времени. Ключ полностью идентифицирован, если повторное чтение проведено успешно и его данные совпадают с первым чтением.

Можно говорить о том, что система контроля доступа приобретает дополнительные свойства без какой-либо нагрузки на пользователей, т.е. повышается интеллект системы в целом.

Следует заметить, что однократное чтение данных ключа составляет 5 мС, соответственно два чтения займут 10 мС, что совершенно не будет заметно для пользователя (обычная мышечная реакция человека имеет значение >100 мС). Относительная стоимость системы возрастет ненамного – хороший микроконтроллер стоит около $ 10 и отпадает необходимость в дополнительном программаторе ключей.

Выводы

Проведенные эксперименты с серией из 20 ключей типа DS1990A подтвердили правильность предложенного подхода – значения амплитуд для фазы presence pulse колебались в пределах 10 – 15%, и значения минимальных временных задержек колебались в пределах 5 – 20% для различных ключей.

Разумеется, у этого подхода есть свои недостатки – временные параметры изменяются с течением времени (т.е. на втором году эксплуатации они будут другими, в сравнении с первым) и меняются с изменением температуры внешней среды. Одна-

ко температуру внешней среды может измерять этот же микроконтроллер и корректировать временные тестовые параметры. Компенсацию времени эксплуатации можно компенсировать повторной регистрацией ключей.

Литература

1. Reading and Writing iButtons via Serial Interfaces [Электронный ресурс]. – Режим доступа : http://pdfserv.maxim ic.com/arpdf/AppNotes/app74.pdf.
2. Transmitting Data and Power over a One-Wire Bus [Электронный ресурс]. – Режим доступа : http://pdfserv.maxim-ic.com/arpdf/AppNotes/onewirebus.pdf.
3. Ридико Л. Имитатор электронных ключей iButton [Электронный ресурс] / Л. Ридико // Схемотехника. – 2000. – № 1. – Режим доступа : http://www.dian.ru/pdf/ibutt.pdf.
4. Ридико Л. Электронный замок с ключами iButton [Электронный ресурс] / Л. Ридико, В. Лапицкий. – Режим доступа : http://radiotech.by.ru/Shematic_PCB/DigitalTehniks/touch_mem.htm.
5. Системы авторизации доступа к «1С: Предприятие» [Электронный ресурс]. – Режим доступа : http://www.servicetrend.ru/All/Vn/Razrabotki/Lock.html.
6. НТЛ «ЭлИн» и «Термохрон» [Электронный ресурс]. – Режим доступа : http://www.elin.ru/microlan/TH10.htm.
7. Цыбульник Е.С. Индивидуальная интеллектуальная система быстрого оповещения об экстренных ситуациях в информатизированном обществе / Е.С. Цыбульник, В.Н. Пигуз // Искусственный интеллект. – 2009. – № 4. – С. 457-461.

Є.С. Цибульник, В.М. Пігуз

Інтелектуальний пристрій контролю доступу

У статті пропонується спосіб удосконалення пристрою контролю доступу з електронними ключами типу DS1990A. Реалізація способу дозволяє захистити систему від ключів-клонів і ключів-симуляторів за незначного дорожчання системи в цілому і без додаткового навантаження на користувачів.

He.S. Tsibulnik, V.N. Pigus

Intellectual Control Unit of Access

In article the way of improvement of a control unit of access with electronic keys of type DS1990A is offered. Realisation of a way allows to protect system from keys-clones and keys-simulators at insignificant rise in price of system as a whole and without additional loading on users.

Статья поступила в редакцию 02.04.2010.